Discrete Mathematics 37 (1981) 1–18
North-Holland Publishing Company

SOME HOWELL DESIGNS OF PRIME SIDE II

B.A. ANDERSON and P.A. LEONARD

Department of Mathematics, Arizona State University, Tempe, AZ 85281, USA

Received 25 March 1980
Revised 14 October 1980

In part I of this paper we showed that for any pair (m, r) of positive integers, r odd, there is a positive integer $N_1(m, r)$ such that if p is a prime, $p = 2^m rs + 1 > N_1(m, r)$, r, s odd positive integers, then Howell Designs of all types $H^*(p, 2n)$, $p + 1 \leq 2n \leq 2p - 2s$ exist. We now verify that under the same hypotheses (except that $(m, r) = (1, 1)$ is not allowed), there is a positive integer $N_2(m, r)$ such that if $p = 2^m rs + 1 > N_2(m, r)$, then Howell Designs of all types $H^*(p, 2n)$, $2p - 2s \leq 2n \leq 2p - 6$ exist. Since designs of type $H^*(p, 2p - 4)$ and $H^*(p, 2p)$ are known to exist for $p \geq 7$, it follows that if $p = 2^m rs + 1 > N(m, r) = \max\{N_1(m, r), N_2(m, r)\}$, then Howell Designs of all types $H^*(p, 2n)$, except possibly type $H^*(p, 2p - 2)$, exist. When this is the case, we say that almost all $H^*(p, 2n)$ exist. As in part I, the method of construction appears to be much better than the general bounds obtained. We are able to show that $N(2, 1) = 5$. Thus, if $5 < p = 4s + 1$, s odd, then almost all $H^*(p, 2n)$ exist. Evidence is presented to show that $N(1, 3)$ is almost certainly 1. In particular, if $p = 6s + 1 < 1000$, s odd, then almost all $H^*(p, 2n)$ exist.

1. Introduction

Suppose X is a set such that $|X| = 2n$. A *Howell Design* on X of type $H(s, 2n)$ consists of a square array of side s such that

(1) each cell either is empty or contains an unordered pair of elements taken from X,

(2) each element of X appears exactly once in each row and each column of the array, and

(3) each unordered pair appears in at most one cell of the array.

It is easy to see that existence requires $n \leq s \leq 2n - 1$. A Howell Design on X of type $H(s, 2n)$ is said to be of type $H^*(s, 2n)$ if there is some set $Y \subset X$ such that $|Y| = 2n - s$ and no pair of elements of Y occupy any cell of the design.

In this paper we are primarily concerned with the existence question for Howell Designs of odd side; for background on this problem see [1, 5, 7, 8]. Worth mentioning here is the currently plausible conjecture that, except for design types $H(3, 4)$, $H(5, 6)$ and $H(5, 8)$, which are known not to exist, Howell Designs of all types $H(s, 2n)$, s odd, exist.

It is known [7] that designs of type $H(s, 2s - 2)$, s odd, can not be constructed by the "starter-adder" methods employed in this paper. Thus we establish the following convention. If s is an odd positive integer, $s \geq 7$, the statement that

0012-365X/81/0000–0000/$02.50

almost all $H^*(s, 2t)$ exist means that if $s+1 \leq 2t \leq 2s-4$ or $2t = 2s$, then there is a Howell Design of type $H^*(s, 2t)$.

The following statement and multiplication theorem from [1] indicate why we are interested in Howell Designs of prime side.

H1. If $p \geq 7$ is a prime, then almost all $H^*(p, 2n)$ exist.

Theorem 1 [1]. *If* H1 *holds and* s *is an odd positive integer such that* $7 \leq s = 3^a 5^b k$, $2, 3, 5 \nmid k$, $a, b \geq 0$ *and* $a+b \neq 1$, *then almost all* $H^*(s, 2n)$ *exist.*

For results in case $a+b=1$ above, see [1, 3, 4, 5]. Clearly it would be very useful to be able to verify H1. The major result of [5] is

Theorem 2 [5]. *Suppose* m *is a positive integer,* r *and* s *are odd positive integers and* $p = 2^m rs + 1$ *is a prime. There is a positive integer* $N_1(m, r)$ *such that if* $p > N_1(m, r)$, *then designs of all types* $H^*(p, 2n)$, $p+1 \leq 2n \leq 2p-2s$ *exist.*

Note that if $(m, r) = (1, 1)$, the resulting special case of Theorem 2 only says that certain Room Squares [8] exist. The major result of this paper is

Theorem 3. *Suppose* m *is a positive integer,* r *and* s *are odd positive integers,* $(m, r) \neq (1, 1)$ *and* $p = 2^m rs + 1$ *is a prime. There is a positive integer* $N_2(m, r)$ *such that if* $p > N_2(m, r)$, *then designs of all types* $H^*(p, 2n)$, $2p-2s \leq 2n \leq 2p-6$ *exist.*

If Theorems 2 and 3 are combined with [7, Theorems 1 and 12] we see that in each case $(m, r) \neq (1, 1)$, eventually almost all types of designs exist.

Generally, the bounds obtained appear to be quite poor indicators of the power of the method. In [5] certain ad hoc procedures and computer testing were used to establish that $N_1(2, 1) = 5$. We are able to use similar methods now to conclude $N_2(2, 1) = 5$. Thus, if $5 < p = 4s+1$, s odd and p prime, then almost all $H^*(p, 2n)$ exist. As in [5] we do not make exhaustive tests in the $(m, r) = (1, 3)$ case but we do show that if $p = 6s+1 < 1000$, s odd and p prime, then almost all $H^*(p, 2n)$ exist.

2. The construction

The concept that is the foundation for this paper as well as [1, 5] is as follows.

Definition 1. Suppose G is a finite Abelian group of odd order written additively and X is a partition of G into singletons S_X and doubletons D_X. We will say that X is a *splitting starter* if and only if

(i) $\{a, b\}, \{c, d\}$ distinct elements of D_X implies $a-b \neq \pm(c-d)$,

(ii) $A : X = S_X \cup D_X \to G$ defined by
(α) $\{s\} \in S_X$ implies $A\{s\} = -2s$ and
(β) $\{a, b\} \in D_X$ implies $A\{a, b\} = -(a+b)$

is an injection.

It is known [5] that a splitting starter X on G yields a Howell Design of type $H^*(|G|, |G| + |S_X|)$. Moreover, it is often possible to "uncouple" a doubleton of X, make a new splitting starter for G with two additional singletons, and thus realize a new type of Howell Design. We assume the reader has access to [1, 5] where the details of the uncoupling process, and its relationship to the digraph Δ_X associated with X, are discussed.

In [5] the presence of long cycles in Δ_X was seen as an obstruction to iteration of the uncoupling process. In this paper, we show that splitting starters whose associated digraphs consist of long cycles can often be changed slightly so that the new digraph contains weak components that consist of a short cycle and a long path. This is exactly what one wants to construct many Howell Designs of the same side. We begin by considering two examples. The ideas in the examples will then be generalized to give the basic construction.

We will use $K = \mathrm{GF}[p^n]$ to denote the finite field of p^n elements. If $p^n = 2^m rs + 1$, r, s odd, let Y denote the subgroup of order s of the multiplicative group K^* of K, let R be a set of coset representatives of Y and if $\hat{R} \subset R$ is partitioned into a set P of unordered pairs,

$$YP = \{\{ya, yb\} : \{a, b\} \in P, y \in Y\}.$$

If x is a generator of K^*, we will denote the cosets of Y as follows. For $0 \leq i < 2^m r$

$$C_i = \{x^{2^m r t + i} : 0 \leq t < s\}.$$

Thus $Y = C_0$. The notation "$u \to v$" will be used to denote an edge of the digraph associated with a splitting starter.

Now, suppose $p = 37 = 4 \cdot 1 \cdot 9 + 1$, $K = \mathrm{GF}[37]$ and Y is the multiplicative subgroup of K^* of order 9. Then $x = 2$ is a primitive root and if $P = \{\{1, 31\}\}$, one easily checks (or uses [5, Theorem 6]) that

$$YP = \{\{1, 31\}, \{16, 15\}, \{34, 18\}, \{26, 29\}, \{9, 20\}, \{33, 24\}, \{10, 14\}, \{12, 2\}, \{7, 32\}\}$$

is D_X for a splitting starter X on $(K, +)$. The digraph associated with YP, Δ_{YP}, is the 9-cycle

$$5 \to 35 \to 23 \to 13 \to 17 \to 8 \to 19 \to 22 \to 6 \to 5.$$

Suppose we try to modify the digraph Δ_{YP} by changing what happens at the vertex 5. If two edges were to emanate from 5, they would be the given one $5 \to -2 \cdot 1 \equiv 35 \pmod{37}$ and $5 \to -2 \cdot 31 \equiv 12 \pmod{37}$. Can we change the digraph by adding the edges $5 \to 12 \to 6$? We would need a pair $\{x, y\}$ such that

$\pm(x+y) = 12$ and $\pm(x-y) = \pm 6$. Since all pairs of YP have differences in $C_0 \cup C_2$ and $6 \in C_3$, the difference is new. Digraphs for splitting starters are contrafunctional (all vertices have indegree one [1]) so that the addition of the edge $12 \to 6$ means that $22 \to 6$ must be deleted. Therefore uncouple the pair $\{34, 18\}$. But this associates 34 with the vertex 6. Thus, we look for an element z such that

(i) $34 + z \equiv 25 \pmod{37}$,

(ii) $34 - z = \pm 6$,

(iii) $z \notin C_0 \cup C_1$, so that z is not in any pair of YP.

A straightforward computation shows that $z = 28$ satisfies these conditions. All that we have really done is to replace the pair $\{34, 18\}$ of X with the pair $\{34, 28\}$. It is easy to see that this new family of pairs is D_W for a splitting starter W on $(K, +)$. Furthermore Δ_W is a 3-cycle $5 \to 12 \to 6 \to 5$ and a 6-path $5 \to 35 \to 23 \to 13 \to 17 \to 8 \to 19$. Thus the uncoupling process can be used with W to construct all $H^*(37, 2n)$, $56 \leqslant 2n \leqslant 68$ or $2n = 74$. Much more can be done with this example. If we extend P to $Q = \{\{1, 31\}, \{3, 22\}\}$, it turns out that YQ is a strong starter (hence splitting starter) on $(K, +)$ whose digraph Δ_{YQ} is the 9-cycle of Δ_{YP} with a 1-path added to each vertex. Thus YQ can be used with the uncoupling process to build all $H^*(37, 2n)$, $38 \leqslant 2n \leqslant 56$. When we put these two ideas together we see that if we start with YQ, uncouple down to YP and modify to W we can construct all $H^*(37, 2n)$, $38 \leqslant 2n \leqslant 68$ or $2n = 74$.

If the above example could be generalized to all primes p, $p \geqslant 7$, H1 would follow. We show that if $p \neq 2q + 1$, q prime, then the above example can be generalized asymptotically.

The second example, which we exhibit in a somewhat different form, is as follows.

Suppose $p = 29 = 4 \cdot 1 \cdot 7 + 1$, $x = 2$ and Y is the multiplicative subgroup of K^* of order 7. If $P = \{\{1, 2\}\}$, then

$$YP = \{\{1, 2\}, \{16, 3\}, \{24, 19\}, \{7, 14\}, \{25, 21\}, \{23, 17\}, \{20, 11\}\}$$

is D_X for a splitting starter X on (GF[29], +) whose associated digraph Δ_X is the 7-cycle

$$26 \to 27 \to 18 \to 12 \to 8 \to 15 \to 10 \to 26.$$

The first row of the following Table 1 includes the image of the "adder" $A[X]$ and the second row has the elements of $X = S_X \cup D_X$ placed in the same column as the appropriate adder element. We could pick any vertex of Δ_X to make the modification, but with the table in the given form, it is helpful to pick vertex 12. Since $-2 \cdot 21 \equiv 16 \pmod{29}$, we try to add the edges $12 \to 16 \to 18$ to the digraph. Note that no pair of YP yields the differences ± 2. This means that we may attempt the modification by uncoupling $\{20, 11\}$ and this is done in the third row

Table 1

0	28	27	26	25	24	23	22	21	20	19	18	17	16
0	15	11, 20	1, 2				18	4		5	17, 23	6	
0	15		1, 2				18	4		5	17, 23, 20	6	
0	15		1, 2				18	4		5	17, 23	6	20, 22

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
19, 24	22	8	21, 25	9	3, 16	10	7, 14		26	12	27	13	28	
19, 24	22	8	21, 25	9	3, 16	10	7, 14	11	26	12	27	13	28	
19, 24		8	21, 25	9	3, 16	10	7, 14	11	26	12	27	13	28	

of the table. It follows that 20 must be paired with z such that

(i) $20+z \equiv 13 \pmod{29}$,

(ii) $20-z = \pm 2$,

(iii) $z \notin C_0 \cup C_1$, so that z is not in any pair of YP.

The last row of the table gives the new splitting starter W with $22 = z$. As expected, Δ_W is a 3-cycle joined to a 4-path.

Definition 2. Suppose K is a finite field, x is a generator of K^*, Y is a multiplicative subgroup of K^* and the cosets $\{C_i\}$ of Y are as previously defined. A *coset quadruple* is an ordered collection (C_u, C_v, C_w, C_z) of cosets of Y. Ordinarily we will use the notation (u, v, w, z) for the coset quadruple (C_u, C_v, C_w, C_z). A coset quadruple (u, v, w, z) is realized by a *basic field quadruple* $(a, a+1, a+2, a+1-4^{-1}a^2)$ if there is an a in K^* such that $a \in C_u$, $a+1 \in C_v$, $a+2 \in C_w$ and $a+1-4^{-1}a^2 \in C_z$.

It will be useful to establish the following notational conveniences. Suppose $p = 2^m rs + 1 = 2ns + 1$ is a prime, x is a generator of the associated K^* and $\alpha = (u, v, w, z)$ is a coset quadruple. Then $e_i = e(\alpha, i)$ is the element of α in position i. Z_{2n} will denote the cyclic group on $2n$ elements, written additively, and if $a_1, \ldots, a_j \in Z_{2n}$, then $\overline{a_1, \ldots, a_j} = Z_{2n} \setminus \{a_1, \ldots, a_j\}$.

We will be interested in families of coset quadruples.

Definition 3. Suppose $p = 2^m rs + 1 = 2ns + 1$ is a prime, K, x, Y and $\{C_i\}$ are related to p as above and $-2 \in C_k$. We define two families of coset quadruples. Arithmetic on the coset labels is mod $2n$.

$F(n, k)$ is the collection of coset quadruples α such that

(1) $e(\alpha, 1) \notin \{k, k+n\}$,

(2) $e(\alpha, 2) \neq 0$,

(3) $e(\alpha, 3) = k+n$,

(4) $e(\alpha, 4) \notin \{0, e(\alpha, 2)\}$

In a more compact notation

$$F(n, k) = \langle \overline{k, k+n} ; \overline{0} ; k+n ; \overline{0, e_2} \rangle.$$

$G(n, k)$ is the collection of coset quadruples β such that

(1) $e(\beta, 1) \notin \{k+e(\beta, 2), k+n+e(\beta, 2)\}$,

(2) $e(\beta, 2) \neq 0$,

(3) $e(\beta, 3) = k+n+e(\beta, 2)$,

(4) $e(\beta, 4) \notin \{e(\beta, 2), 2e(\beta, 2)\}$

Thus

$$G(n, k) = \langle \overline{k+e_2, k+n+e_2} ; \overline{0} ; k+n+e_2 ; \overline{e_2, 2e_2} \rangle.$$

Theorem 4. *Suppose $p = 2^m rs + 1 = 2ns + 1$ is a prime with r, s odd and $n \geq 2$; suppose x is a generator of the associated $K^*, -2 \in C_k$ and $a^* = (a, a+1, a+2, a+1-4^{-1}a^2)$ is a basic field quadruple. If a^* realizes a coset quadruple of*

(i) *$F(n, k)$ and $8(a+2)^{-3} \neq 1$, or*

(ii) *$G(n, k)$ and $8(a+2)^{-3}(a+1)^3 \neq 1$,*

then Howell Designs of all types $H^*(p, 2n)$, $2p-2s \leq 2n \leq 2p-6$ exist.

Proof. We consider the case of a^* realizing a coset quadruple α of $F(n, k)$. The argument for the other case is similar. The plan will be to define a splitting starter whose digraph is such that the uncoupling process will give the required types of designs.

Let $P = \{\{1, a+1\}\}$. Since a^* realizes a coset quadruple α of $F(n, k)$, it follows that $a+1 \in C_l$, $l \neq 0$ and $a+2 \in C_{k+n}$. Thus by [5, Theorem 6], YP is D_X for a splitting starter X on K. The fact that $-1 \in C_n$ implies that $-(a+2) \in C_k$ and hence that the vertex set of Δ_X, denoted V_X, is C_k. If $\{y, y(a+1)\}$ is a pair of YP, then there are two possibilities for edges of Δ_X emanating from $-y(a+2)$; $-y(a+2) \rightarrow -2y$ and $-y(a+2) \rightarrow -2y(a+1)$. Since $-2y \in C_k$, the edge set of Δ_X is

$$E_X = \{-y(a+2) \rightarrow -2y : y \in Y\}.$$

If $\{y_1, y_1(a+1)\} \in YP$ and $-y_1(a+2) \rightarrow -2y_1 \in E_X$, then there is a y_2 in Y such

that $\{y_2, y_2(a+1)\} \in YP$ and $-2y_1 = -y_2(a+2)$. Note, therefore, that given a vertex of Δ_X and its associated pair, one can move to the next vertex and associated pair in the digraph by multiplying by $2(a+2)^{-1}$ and $1 \neq 2(a+2)^{-1} \in Y = C_0$. Thus

$$2(a+2)^{-1}(-y_1)(a+2) = -2y_1$$

and

$$2(a+2)^{-1}\{y_1, y_1(a+1)\} = \{y_2, y_2(a+1)\}.$$

Hence, it is clear that E_X is a union of disjoint cycles and that the multiplicative order of $2(a+2)^{-1}$ controls the length t and the number s/t of cycles in Δ_X. Note that since $8(a+2)^{-3} \neq 1$, the odd positive integer t is greater than 3.

We now define a modification of the splitting starter X. Fix an element y of Y. We shall modify the t-cycle of Δ_X that contains the vertex $v_0 = -y(a+2)$, corresponding to the pair $\{y, y(a+1)\}$. The t-cycle contains the edges $v_{t-2} \to v_{t-1} \to v_0$. Since multiplying by $2(a+2)^{-1}$ allows us to follow the arrows in Δ_X, multiplying by $2^{-1}(a+2)$ traces the t-cycle in the reverse direction. Thus v_{t-1} and its associated pair are

$$v_{t-1} = -2^{-1}y(a+2)^2; \quad \{2^{-1}(a+2)y, 2^{-1}(a+2)y(a+1)\}$$

and v_{t-2} and its associated pair are

$$v_{t-2} = -4^{-1}y(a+2)^3; \quad \{4^{-1}(a+2)^2y, 4^{-1}(a+2)^2y(a+1)\}.$$

The change is as follows. Replace the pair R_1 associated with v_{t-2} by the pair

$$R_2 = \{4^{-1}(a+2)^2y, (a+1-4^{-1}a^2)y\}.$$

(In the other case involving $G(n, k)$, replace the pair

$$R_1 = \{4^{-1}(a+2)^2(a+1)^{-2}y, 4^{-1}(a+2)^2y(a+1)^{-1}\}$$

of YP by the new pair

$$R_2 = \{(a+1-4^{-1}a^2)(a+1)^{-1}y, 4^{-1}(a+2)^2y(a+1)^{-1}\}.)$$

This is equivalent to uncoupling the pair associated with v_{t-2} and then coupling $4^{-1}(a+2)^2y$ with the element $z = (a+1-4^{-1}a^2)y$. The new pair formed will have sum $2y(a+1)$ and differences $\pm 2^{-1}ya^2$. It is easy to see that since a^* realizes a coset quadruple α of $F(n, k)$, the new pair will not have the same differences as any pair of YP and z is not a member of the cosets paired in YP. Thus, it is clear, using Definition 1, that $(YP \cup R_2) \setminus R_1$ is D_X for a splitting starter X' on K.

The new pair introduces a new vertex $\hat{v} = -2y(a+1)$ and the new edges $v_0 \to \hat{v}$, since v_0 corresponds to $\{y, y(a+1)\}$, and $\hat{v} \to v_{t-1}$, since $v_{t-1} = -2 \cdot 4^{-1}(a+2)^2y$. The vertex v_{t-2}, and the two edges containing it, disappear. Thus, changing X to X' transforms the t-cycle containing v_0 to the 3-cycle $v_0 \to \hat{v} \to v_{t-1} \to v_0$ and a "tail", namely the original $(t-3)$-path from v_0 to v_{t-3}. The process is completed by picking a vertex v_0 from each of the t-cycles that make up Δ_X, and modifying that

cycle in the indicated fashion. Since each choice of v_0 involves a different y, the elements z differ from one another as do the differences associated with the new pairs. The process therefore results in D_W for a splitting starter W. After completing the modification, the graph Δ_W is a collection of "tadpoles", and the uncoupling process [1] can be used to build the required types of designs, since $t \geq 5$.

3. Utility of the construction

In this section we show that the method of construction described in Theorem 4 works asymptotically. In addition, we show that, in certain cases, variations of the construction and bounding procedure yield very strong results. For both purposes, we employ counting arguments which involve character sums and deep estimates due to Perel'muter for the sums in question. The treatment parallels that in [5], to which we refer for appropriate details. We shall, however, present the main lines of the argument here for completeness.

Let $K = \mathrm{GF}[p^n]$, where $p^n = cd + 1$ is an odd prime power and let x be a fixed generator of the associated K^*. Let χ be the character of order c on K^* defined by

$$\chi(x^i) = \omega^i, \qquad 0 \leq i \leq p^n - 2$$

where $\omega = \exp(2\pi i/c)$. Then the sets

$$C_u = \{y: y \in K^* \quad \text{and} \quad \chi(y) = \omega^u\}, \quad 0 \leq u \leq c-1,$$

are the cosets in K^* of the subgroup $Y = C_0$ consisting of the c-th powers.

Definition 4. Let $\chi(0) = 0$, and let $\chi^0(0) = 0$ in sums involving χ^i. For $b \in K$ and $0 \leq u \leq c-1$, let

$$S_u(b) = \sum_{i=0}^{c-1} \omega^{-iu} \chi^i(b).$$

Lemma 1 [5]. *For $b \in K$ we have*

$$S_u(b) = \begin{cases} c, & \text{if } b \in C_u, \\ 0, & \text{otherwise.} \end{cases}$$

The lemma just stated leads to a method of wide applicability to constructions of the sort discussed here. We outline this method in more generality than we require here to indicate its usefulness.

Suppose $R(x) = \prod_{i=1}^{s} P_i(x) \in K[x]$. Let $(u_1, \ldots, u_s)$ be any ordered s-tuple of integers all in $[0, c-1]$. We require an expression for the number A of elements a in K for which $1 \leq i \leq s$ implies $P_i(a) \in C_{u_i}$.

Lemma 2.

$$c^s\Lambda = \sum_{a\in K}\prod_{i=1}^{s} S_{u_i}(P_i(a))$$
$$= \sum_{0\le j_1,\ldots,j_s\le c-1} \omega^{-\sum_{i=1}^{s} j_i u_i} \sum_{a\in K}\prod_{i=1}^{s} \chi^{j_i}(P_i(a)).$$

Proof. This is immediate from Lemma 1.

Consider the sums $\sigma(j_1,\ldots,j_s)=\sum_{a\in K}\prod_{i=1}^{s}\chi^{j_i}(P_i(a))$ which arise in Lemma 2. Each σ can be compared with the sum $\tau(j_1,\ldots,j_s)=\sum_{a\in K}\chi(\prod_{i=1}^{s}P_i^{j_i}(a))$, where if j_i is zero the corresponding $P_i^0(a)$ is taken to be 1 for all a in K. Each sum τ differs from the corresponding σ only in terms involving zeros of the polynomials $P_i(a)$, $1\le i\le s$. In particular $\tau(0,\ldots,0)=p^n$ and $\sigma(0,\ldots,0)=p^n-h$, where h is the number of a in K such that for at least one i, $P_i(a)=0$. If $R(x)$ is "reduced" [5, 9], the results of Perel'muter apply to give estimates for the remaining sums $\tau(j_1,\ldots,j_s)$, $(j_1,\ldots,j_s)\ne(0,\ldots,0)$ so that in each case

$$|\tau(j_1,\ldots,j_s)|\le M\sqrt{p^n}+1.$$

M can be taken to be $\sum_{i=1}^{s}\deg P_i(x)-1$. These estimates, together with the evaluation of $\sigma(0,\ldots,0)$ give the inequality

$$|c^s\Lambda-p^n|\le J\sqrt{p^n}+L$$

for suitable constants J and L. This implies

$$c^s\Lambda\ge p^n-J\sqrt{p^n}-L$$

and so Λ tends to infinity with p^n. In particular, any desired value for Λ (e.g. $\Lambda\ge 5$) is achieved for $p^n\ge T(c)$, with the size of $T(c)$ determined by the values of J and L.

For a fixed c, the value for $T(c)$ obtained is quite large, owing to the presence of c^s character sums, each estimated separately. Moreover, $T(c)$ grows with c. We have, then, asymptotic results that fall far short of what is desired. On the other hand, when these methods are applied to the construction of Howell Designs, they appear to give designs far sooner, for a fixed c, than the estimates enable us to guarantee.

The main result is the following

Theorem 5. *Suppose $K=\mathrm{GF}[p^n]$, p odd, $p^n=cd+1$, let x be a fixed generator of K^*, let χ be the character of order c on K^* defined as previously and let C_0 be the multiplicative subgroup of order d of K^*. For $i=1,2,3$ there is a positive integer $T_i(c)$ such that if $p^n>T_i(c)$, then the statement* (i) *below holds.*

(1) *Any particular coset quadruple (u,v,w,z) can be realized by a basic field quadruple beginning with a such that $8(a+2)^{-3}\ne 1$.*

(2) *Any particular coset quadruple (u,v,w,z) can be realized by a basic field quadruple beginning with a such that $8(a+2)^{-3}(a+1)^3\ne 1$.*

(3) *All coset quadruples can be realized by basic field quadruples.*

Proof. Clearly (3) follows from (1) or (2) since there are only a finite number of coset quadruples. For u, v, w, z fixed, $0 \leq u, v, w, z \leq c-1$, let Λ denote the number of a in K for which the basic field quadruple beginning with a realizes the coset quadruple (u, v, w, z). The equation $y^3 = 1$ has at most three solutions in K, one of them being $y = 1$. Now $2(a+2)^{-1} = 1$ if and only if $a = 0$ and $2(a+2)^{-1}(a+1) = 1$ if and only if $a = 0$. We can therefore assume that an a exists to satisfy (1) [or (2)] if we can show $\Lambda \geq 3$. Apply the argument outlined above with $P_1(x) = x$, $P_2(x) = x+1$, $P_3(x) = x+2$ and $P_4(x) = x+1-4^{-1}x^2$. For each $(i, j, k, l) \neq (0, 0, 0, 0)$, consider the sum

$$\tau(i, j, k, l) = \sum_{a \in k} \chi(P_1^i(a) \cdot P_2^j(a) \cdot P_3^k(a) \cdot P_4^l(a)).$$

The function $R(x) = P_1^i(x) \cdot P_2^j(x) \cdot P_3^k(x) \cdot P_4^l(x)$ will be "reduced" (see [5, 9]) unless the g.c.d. of i, j, k, l, and c is b, with $b > 1$. In this case we have

$$\chi(R(x)) = \chi([R_0(x)^{c/b}]^b) = \chi^b([R_0(x)]^{c/b})$$

and we replace χ by χ^b, which has order c/b. The new argument $[R_0(x)]^{c/b}$ is then "reduced" (relative to χ^b).

In all cases where the argument is "reduced", the estimates of Perel'muter apply. Thus, for each $(i, j, k, l) \neq (0, 0, 0, 0)$ we have $|\tau(i, j, k, l)| \leq M\sqrt{p^n} + 1$ for some M. As the above discussion has shown, this implies the existence of $T_1(c)$ with the property that $\Lambda \geq 3$ for all $p^n = cd + 1 > T_1(c)$. This completes the proof of the theorem.

Clearly Theorems 4 and 5 combine to yield a proof of Theorem 3.

It is possible, for a fixed c, to carry out the estimations of the $\tau(i, j, k, l)$ in detail, and thereby arrive at a value for $T_i(c)$. Although the estimates for the individual terms are sharp, the effect of estimating $c^4 - 1$ terms separately is to produce astronomical values for $T_i(c)$. For example, if $c = 4$ the above process will yield a bound on the order of 100,000.

We are now ready to undertake a careful analysis of the case p prime, $p = 4s + 1$, s odd. For such a prime p, we will always assume a primitive root x is chosen so that $-2 \in C_3$. As in Theorem 4, we are interested in the coset quadruples (C_u, C_v, C_w, C_z), denoted as before by (u, v, w, z), that can be realized by a basic field quadruple $(a, a+1, a+2, a+1-4^{-1}a^2)$. We know that if certain coset quadruples can be realized by a basic field quadruple beginning with a and $8(a+2)^{-3} \neq 1$ [or $8(a+2)^{-3}(a+1)^3 \neq 1$, depending on the coset quadruple], then certain types of Howell Designs exist. It will suffice to use eight of the coset quadruples that arise from Theorem 4 in the special case $p = 4s + 1$. These quadruples can be combined in an argument that will reduce the bound $N_2(2, 1)$ to 2809, a substantial improvement from 100,000.

Lemma 3. *If p is a prime, $p \equiv 5 \pmod 8$ and $a \in \mathrm{GF}[p]$, then $a + 1 - 4^{-1}a^2 \neq 0$.*

Proof. It is easy to see that $a+1-4^{-1}a^2=0$ has a solution if and only if 2 is a quadratic residue mod p and this is false when $p\equiv 5 \pmod 8$.

Lemma 4. *If $p=4s+1$ s odd and any of the coset quadruples $(0,2,1,1)$, $(0,2,1,3)$, $(2,2,1,1)$ or $(2,2,1,3)$ can be realized by a basic field quadruple beginning with a such that $8(a+2)^{-3}\neq 1$, then Howell Designs of all types $H^*(p,2n)$, $2p-2s\leqslant 2n\leqslant 2p-6$ exist.*

Proof. Recall that

$$F(n,k)=\langle \overline{k,k+n};\bar{0};k+n;\overline{0,e_2}\rangle.$$

We have agreed to choose x so that $k=3$ and clearly $n=2$. Thus

$$F(2,3)=\langle \overline{3,1};\bar{0};1;\overline{0,e_2}\rangle.$$

If $e_2=2$, this reduces to the four coset quadruples listed.

Lemma 5. *If $p=4s+1$, s odd and any of the coset quadruples $(0,2,3,1)$, $(0,2,3,3)$, $(2,2,3,1)$ or $(2,2,3,3)$ can be realized by a basic field quadruple beginning with a such that $8(a+2)^{-3}(a+1)^3\neq 1$, then Howell Designs of all types $H^*(p,2n)$, $2p-2s\leqslant 2n\leqslant 2p-6$ exist.*

Proof. This follows as in Lemma 4 with $F(2,3)$ replaced by $G(2,3)$.

Let N denote the number of a in K such that the basic field quadruple beginning with a realizes one of the eight coset quadruples listed in Lemmas 4 and 5. Let χ denote a character of K^* of order 4, and let $\lambda=\chi^2$ be the quadratic character. In order to realize one of the above coset quadruples, it will suffice to find a such that a is a square, $a+1$ is in C_2 and $a+2$ and $a+1-4^{-1}a^2$ are nonsquares in K^*.

Lemma 6. *Let $S_u(b)$ be as in Lemma 1, for χ a character of order 4 and suppose*

$$T_j(b)=\lambda^0(b)+(-1)^j\lambda^1(b);\quad j=0,1,$$

are the corresponding sums for $\lambda=\chi^2$. Then

$$32N=\sum_{a\in K}T_0(a)S_2(a+1)T_1(a+2)T_1(a+1-4^{-1}a^2)$$

$$=\sum(-1)^{i+k+l}\sum_{a\in K}\chi^i(a)\chi^j(a+1)\lambda^k(a+2)\lambda^l((a-2)^2-8)$$

where the unspecified summation is over all 4-tuples (i,j,k,l) with $0\leqslant i,k,l\leqslant 1$, $0\leqslant j\leqslant 3$.

Proof. This is clear once it is noted that

$$a+1-4^{-1}a^2=-4^{-1}(a^2-4a-4)=-4^{-1}((a-2)^2-8)$$

and that since $p\equiv 1 \pmod 4$, $\lambda^1(-4^{-1})=1$.

By applying estimates to the character sums which appear in the final expression for $32N$ we can obtain

Lemma 7. *Suppose p is a prime $p = 4s + 1$, s odd, and N is defined as above. Then*

$$|32N - p - 3| \leq 50\sqrt{p} + 27.$$

Proof. The result follows from a consideration of the 32 character sums that appear in Lemma 6. Some of these can be evaluated exactly, while others are estimated in various ways. Details are given for six of the 4-tuples (i, j, k, l) to illustrate the techniques employed.

(i) (0, 0, 0, 1)

$$\begin{aligned}
&-\sum_{a\in K} \lambda^0(a)\chi^0(a+1)\lambda^0(a+2)\lambda^1((a-2)^2-8) \\
&= -\left\{\sum_{a\in K} \lambda((a-2)^2-8) - \lambda(-4) - \lambda(1) - \lambda(8)\right\} \\
&= -\left\{\sum_{a\in K} \lambda((a-2)^2-8)\right\} + (1+1-1) \\
&= -(-1)+1 = 2
\end{aligned}$$

since $p \equiv 5 \pmod 8$, using the exact evaluation [6, pp. 147–149] of the sum $\sum_{x\in K} \lambda(f(x))$ when $f(x)$ is a quadratic polynomial.

(ii) (0, 3, 1, 0)

$$\begin{aligned}
&\sum_{a\in K} \lambda^0(a)\chi^3(a+1)\lambda^1(a+2)\lambda^0((a-2)^2-8) \\
&= \left\{\sum_{a\in K} \chi^3(a+1)\lambda(a+2)\right\} - \chi^3(1)\lambda(2) \\
&= \left\{\chi^3(-1)\lambda(1)\sum_{x+y=1} \chi^3(x)\lambda(y)\right\} + 1 \\
&= -(A - 2B_i) + 1 = -A + 2Bi + 1,
\end{aligned}$$

where A, B are determined by $p = A^2 + 4B^2$, $A \equiv 1 \pmod 4$, using explicit evaluations [6, p. 443] for Jacobi sums connected with quartic characters.

(iii) (1, 2, 1, 0)

$$\begin{aligned}
&-\sum_{a\in K} \lambda^1(a)\chi^2(a+1)\lambda^1(a+2)\lambda^0((a-2)^2-8) \\
&= -\sum_{a\in K} \lambda(a(a+1)(a+2)) = -2A
\end{aligned}$$

with A as above, using the explicit evaluation (due to Jacobsthal) of the character sum in question [6, p. 161].

The term (iii) can be combined with (ii) and other terms like (ii) before

estimating. This results in only a slight gain, in this case, over estimating each term, but the technique is frequently useful in giving improvements over term by term estimation.

(iv) (0, 2, 0, 1)

$$-\sum_{a\in K}\lambda^0(a)\chi^2(a+1)\lambda^0(a+2)\lambda^1((a-2)^2-8)$$

$$=\left\{-\sum_{a\in K}\lambda((a+1)((a-2)^2-8))\right\}+\lambda(-4)+\lambda(8)$$

$$=-\sum_{a\in K}\lambda((a+1)((a-2)^2-8))$$

since $p\equiv 5 \pmod 8$. This term can be estimated by $2\sqrt{p}$ by a result of Hasse [6, pp. 145–146], a special case of Weil's estimates.

(v) (0, 3, 1, 1)

$$-\sum_{a\in K}\lambda^0(a)\chi^3(a+1)\lambda^1(a+2)\lambda^1((a-2)^2-8)$$

$$=\left\{-\sum_{a\in K}\chi((a+1)^3(a+2)^2((a-2)^2-8)^2)\right\}+\lambda(2)\lambda(-4).$$

This term is estimated by $3\sqrt{p}+2$, using Perel'muter's result [9] to estimate the character sum involving χ.

(vi) (1, 2, 1, 1)

$$\sum_{a\in K}\lambda^1(a)\chi^2(a+1)\lambda^1(a+2)\lambda^1((a-2)^2-8)$$

$$=\sum_{a\in K}\lambda(a(a+1)(a+2)((a-2)^2-8)),$$

which is estimated by $4\sqrt{p}+1$ using Weil's estimates [6, pp. 145–146] for sums with the quadratic character.

Similar techniques enable us to evaluate or estimate each of the 32 sums that occur. This work is summarized in the following Table 2 where the reference information is coded as follows: I = [6, p. 138], II = [6, pp. 145–146], III = [6, pp. 147–149], IV = [6, p. 161], V = [6, p. 199] and VI = [6, p. 443].

The terms not involving $\sqrt{p}$ are exact values and sum to $p-6A+3$, with A as in (ii) above. The remaining terms sum to a value E with $|E|<44\sqrt{p}+27$. Thus

$$32N = p-6A+3+E$$

and the result follows since $|A|\leq\sqrt{p}$.

It turns out that in order to achieve Howell Design construction we must have $N\geq 5$. This is because the coset quadruples in Lemma 4 are from $F(2,3)$ and those from Lemma 5 are from $G(2,3)$. Thus we wish to find a basic field quadruple beginning with a such that $8(a+2)^{-3}\neq 1$ and $8(a+2)^{-3}(a+1)^3\neq 1$. We have previously noted that $2(a+2)^{-1}=1$ if and only if $a=0$ and that

Table 2

4-Tuple	Estimate or value	Source	4-Tuple	Estimate or value	Source
(0, 0, 0, 0)	$p-3$		(1, 0, 0, 0)	0	I
(0, 0, 0, 1)	2	III	(1, 0, 0, 1)	$2\sqrt{p}+2$	II
(0, 0, 1, 0)	0	I	(1, 0, 1, 0)	2	III
(0, 0, 1, 1)	$2\sqrt{p}$	II	(1, 0, 1, 1)	$2\sqrt{p}+2$	II
(0, 1, 0, 0)	0	V	(1, 1, 0, 0)	$-A-2Bi+1$	VI
(0, 1, 0, 1)	$2\sqrt{p}+3$	[9]	(1, 1, 0, 1)	$3\sqrt{p}+2$	[9]
(0, 1, 1, 0)	$-A-2Bi+1$	VI	(1, 1, 1, 0)	$2\sqrt{p}+1$	[9]
(0, 1, 1, 1)	$3\sqrt{p}+2$	[9]	(1, 1, 1, 1)	$4\sqrt{p}+1$	[9]
(0, 2, 0, 0)	-2	I	(1, 2, 0, 0)	0	III
(0, 2, 0, 1)	$2\sqrt{p}$	II	(1, 2, 0, 1)	$2\sqrt{p}+2$	II
(0, 2, 1, 0)	0	III	(1, 2, 1, 0)	$-2A$	IV
(0, 2, 1, 1)	$2\sqrt{p}+2$	II	(1, 2, 1, 1)	$4\sqrt{p}+1$	II
(0, 3, 0, 0)	0	V	(1, 3, 0, 0)	$-A+2Bi+1$	VI
(0, 3, 0, 1)	$2\sqrt{p}+3$	[9]	(1, 3, 0, 1)	$3\sqrt{p}+2$	[9]
(0, 3, 1, 0)	$-A+2Bi+1$	VI	(1, 3, 1, 0)	$2\sqrt{p}+1$	[9]
(0, 3, 1, 1)	$3\sqrt{p}+2$	[9]	(1, 3, 1, 1)	$4\sqrt{p}+1$	[9]

$2(a+2)^{-1}(a+1)=1$ if and only if $a=0$ so that these possibilities may be discounted. It is clear that if $a, b \in K^*$, $a \neq b$, then

$$2(a+2)^{-1} \neq 2(b+2)^{-1}$$

and

$$2(a+2)^{-1}(a+1) \neq 2(b+2)^{-1}(b+1).$$

Thus, at most four elements of K^* must be avoided.

We use Lemma 7 in the form

$$32N-p-3 \geq -50\sqrt{p}-27,$$

or

$$32(N-4) \geq p-50\sqrt{p}-152.$$

Thus $N>4$, whenever $\sqrt{p}>25+\sqrt{3108}/2$. If we round 3108 up to 3136, it follows that $N>4$ if $\sqrt{p}>53$, that is, if $p>2809$. This allows the remaining cases to be checked individually. The results of those computations are summarized in Table 3.

Theorem 6. *If p is a prime, $5<p=4s+1$, s odd, then Howell Designs of all types $H^*(p, 2n)$, $2p-2s \leq 2n \leq 2p-6$ exist.*

Corollary 1. *If p is a prime, $5<p=4s+1$, s odd, then almost all $H^*(p, 2n)$ exist.*

Proof. This follows from Theorem 6 and [5, Theorem 10].

Table 3

Prime	Root	A	Prime	Root	A	Prime	Root	A
53	2	6	829	2	191	1861	2	1713
61	2	49*	853	2	733	1877	2	64
101	2	64	877	2	798	1901	2	1414
109	6	60	941	2	270	1933	5^{-1}	1592
149	2	120	997	7	984	1949	2	1599
157	5	110	1013	3^{-1}	789	1973	2	411
173	2	43*	1021	10	767	1997	2	408
181	2	55	1061	2	980	2029	2	1208
197	2	6	1069	6^{-1}	761	2053	2	993
229	6	209	1093	5^{-1}	555	2069	2	2007
269	2	151	1109	2	644	2141	2	1408
277	5^{-1}	40	1117	2	999	2213	2	286
293	2	9	1181	7^{-1}	681	2221	2	1721
317	2	6	1213	2	1169	2237	2	2141
349	2	282	1229	2	323	2269	2	2157
373	2	272	1237	2	64	2293	2	1007
389	2	45	1277	2	832	2309	2	752
397	5^{-1}	3	1301	2	492	2333	2	652
421	2	124	1373	2	748	2341	7^{-1}	1024
461	2	323	1381	2	134	2357	2	1133
509	2	216	1429	6^{-1}	675	2381	3	1843
541	2	154	1453	2	524	2389	2	1937
557	2	389	1493	2	869	2437	2	120
613	2	348	1549	2	830	2477	2	1803
653	2	474	1597	11	1230	2549	2	2369
661	2	484	1613	3	1052	2557	2	1895
677	2	136	1621	2	1150	2621	2	1996
701	2	517	1637	2	1107	2677	2	2142
709	2	646	1669	2	1271	2693	2	1985
733	6	569	1693	2	1461	2741	2	441
757	2	155	1709	3^{-1}	729	2749	6^{-1}	240
773	2	96	1733	2	889	2789	2	1963
797	2	227	1741	2	1619	2797	2	1420
821	2	95	1789	6^{-1}	1527			

We need to make several observations about Table 3. First, it is not necessary (by [2]) to consider primes <53. The root listed is chosen so that $-2 \in C_3$. Unless the number is starred, A is the initial element of a basic field quadruple whose first three terms realize the coset triple (2, 2, 3). It is known from previous work [4] that this coset triple can be realized whenever $p \equiv 5 \pmod 8$ and $p \geq 37$. Thus it was natural to test for quadruples from Lemma 5. The table shows that in every case except $p = 61$ and $p = 173$ there is a basic field quadruple beginning with A that realizes either coset quadruple (2. 2, 3, 1) or coset quadruple (2, 2, 3, 3) and has the property that $8(A+2)^{-3}(A+1)^3 \neq 1$. An argument similar to that used in Lemma 4 shows that if either of the coset quadruples (0, 1, 1, 2) or (2, 1, 1, 2) can be realized by a basic field quadruple beginning with A and $8(A+2)^{-3} \neq 1$, then the conclusion of Lemma 4 holds. If $p = 61$, A is the initial element of a basic

Table 4

Prime	Root	Coset	A	D	Coset Quad
67	2	4	59	44	0, 2, 1, 1
79	3	1	14	45	3, 3, 4, 4
103	5	5	47	88	1, 5, 2, 1
127	3	3	92	9	1, 5, 0, 2
139	2	4	117	136	2, 4, 1, 2
151	6	1	36	15	2, 4, 4, 1
163	2	4	126	70	0, 3, 1, 5
199	3	1	14	165	2, 1, 4, 4
211	2	4	129	137	3, 1, 1, 2
223	3	3	58	110	2, 3, 0, 4
271	6	1	112	229	2, 1, 4, 2
283	3	0	25	82	4, 5, 3, 1
307	5	0	296	190	1, 1, 3, 4
331	3	4	53	262	2, 4, 1, 5
367	6	1	355	320	2, 4, 4, 3
379	2	4	289	160	2, 4, 1, 5
439	15	3	248	238	1, 5, 0, 1
463	3	1	79	256	2, 3, 4, 2
487	3	1	79	346	3, 1, 4, 5
499	7	0	341	89	5, 4, 3, 5
523	2	4	126	342	3, 5, 1, 3
547	2	4	126	534	2, 2, 1, 1
571	3	2	241	425	3, 1, 5, 3
607	3	5	332	92	1, 5, 2, 3
619	2	4	564	273	2, 1, 1, 2
631	3	5	249	367	1, 2, 2, 3
643	11	0	626	394	4, 3, 3, 2
691	3	0	136	350	2, 1, 3, 5
727	5	3	356	661	1, 5, 0, 3
739	3	0	263	523	2, 2, 3, 3
751	3	5	599	81	1, 3, 2, 4
787	2	4	126	93	5, 1, 1, 3
811	3	0	25	478	4, 4, 3, 5
823	3	1	614	188	3, 3, 4, 1
859	2	4	126	453	3, 4, 1, 3
883	2	4	243	272	5, 5, 1, 4
907	2	4	126	693	2, 1, 1, 4
919	7	3	235	904	4, 4, 0, 2
967	5	5	23	617	3, 3, 2, 2
991	6	1	783	869	3, 2, 4, 1

field quadruple that realizes the (2, 1, 1, 2) coset quadruple and $8(A+2)^{-3} \neq 1$. If $p = 173$, A is the initial element of a basic field quadruple that realizes the (0, 1, 1, 2) coset quadruple and $3 \nmid 172$ so that $8(A+2)^{-3} \neq 1$.

Clearly one can attempt to apply the above methods to other situations and, in particular, to the "6-coset" case. In this paper we content ourselves with making computations (similar to these for $N_1(1, 3)$ in [5]) to show that the statement $N_2(1, 3) = 1$ is almost certainly true. The results of those computations are summarized in Table 4 and lead to

Theorem 7. *If p is a prime, $p = 6s + 1 < 1000$, s odd, then Howell Designs of all types $H^*(p, 2n)$, $2p - 2s \leq 2n \leq 2p - 6$ exist.*

Corollary 2. *If p is a prime, $p = 6s + 1 < 1000$, s odd, then almost all $H^*(p, 2n)$ exist.*

Proof. This follows from Theorem 7 and [5, Theorem 11].

As mentioned above, Table 4 contains the information necessary to verify Theorem 7. First, by [2] we may restrict our attention to primes p of the proper form such that $p \geq 67$. If the coset column of Table 4 contains the integer k, then with respect to the given primitive root, $-2 \in C_k$. A and D are the initial and final elements of a basic field quadruple that realizes the given coset quadruple and is such that $8(A+2)^{-3} \neq 1$. Recall that

$$F(3, k) = \langle \overline{k, k+3}\,;\, \overline{0}\,;\, k+3\,;\, \overline{0, e_2} \rangle.$$

Thus each $F(3, k)$ contains 80 coset quadruples. It may be verified that every coset quadruple of Table 4 is in $F(3, k)$, for the appropriate k, so that Theorem 7 is a consequence of Theorem 4.

4. Final remarks

The large number of coset quadruples in $F(n, k)$ and $G(n, k)$ and the computational experience outlined in Tables 3 and 4 make it intriguing to speculate on the real power of Theorem 4. Note that Theorem 5 tells us, in some sense, that all coset quadruples have an equal chance to be realized. Suppose we adopt this point of view and neglect the possibility that if $a+2 \in K^*$, then $a, a+1$ or $a+1-4^{-1}a^2$ could be zero. If we consider the family $F(n, k)$, an easy computation shows that if $a+2 \in C_{k+n}$, the probability that $(a, a+1, a+2, a+1-4^{-1}a^2)$ realizes an element of $F(n, k)$ is

$$(2n^3 - 5n^2 + 4n - 1)/2n^3.$$

If $n = 3$ this probability becomes 20/54, a value that appears to hold up very well in actual computation. Similar reasoning would seem to indicate that Theorem 4 should give designs almost immediately for any value of n.

Finally we note a recent result on designs of type $H(s, 2s-2)$,s odd. The paper [10] shows that these designs always exist if $s \geq 7$. Thus, it is possible to say that in many cases, all types of designs of side p, p prime, exist. We still can't say that all $H^*(p, 2n)$ exist in these cases because only one example of type $H^*(p, 2p-?)$ is known.

References

[1] B A. Anderson, Starters, digraphs and Howell designs, Utilitas Math. 14 (1978) 219–248.
[2] B.A. Anderson, Howell designs from Room squares, in: Proceedings of the 2nd Caribbean Conference in Combinatorics and Computing, University of the West Indies, Barbados (1977) 55–62.
[3] B.A. Anderson, A note on Howell designs, Utilitas Math. 18 (1980) 41–49.
[4] B.A.Anderson and K.B. Gross, Asymptotic multiplication of Howell designs by 3, Ars Combinatoria, 10 (1980) 3–17.
[5] B.A.Anderson, K.B. Gross and P.A. Leonard, Some Howell designs of prime side, Discrete Math. 28 (1979) 113–134.
[6] H. Hasse, Vorlesungen über Zahlentheorie (Springer-Verlag, Berlin/Göttingen/Heidelberg, 1950).
[7] S.H.Y Hung and N.S. Mendelsohn, On Howell designs, J. Combinatorial Theory (Ser. A) 16 (1974) 174–198.
[8] R.C. Mullin and W.D. Wallis, The existence of Room squares, Aequationes Math. 13 (1975), 1–7.
[9] G.I. Perel'muter, On certain sums of characters, Usp. Math. Nauk. 18 (1963) 145–149.
[10] P.J. Schellenberg, D.R. Stinson, S.A. Vanstone and J.W. Yates, The existence of Howell designs of side $n+1$ and order $2n$, to appear.